

09/503205

Abstract of the Disclosure

If a condition which can be intuitively hit upon, such as the bit length of a prime number or an extension degree is designated, the expression data of a finite field corresponding to the condition can be automatically generated, and a finite field operation can be performed using the expression data.